TABLE OF CONTENTS

## INTRODUCTION

The Office of Internal Audit performed an audit of the Local Accounting System Replacement (LASR). The objectives of our audit were:

- To assess whether the general system controls that support the use and operation of the LASR application were adequate to provide consistent and reliable operation. General Controls are the controls over design, implementation, security, and use of computer programs and files.
- To assess whether the application controls are adequate to ensure accurate, complete, and approved data, and to prevent unauthorized processing.

## BACKGROUND

LASR is the accounting system used in the FIA local offices. LASR was designed to be operated much like an individual stand-alone accounting system that supports the financial transactions within each local office. There are, however, some centralized functions and reporting.

Each FIA local office inputs source information, prints checks, and maintains its general ledger. Each local office determines its own internal control structure and reconciliation process to ensure the accuracy and integrity of its data in LASR.

The Local Office Liaison Section of the Bureau of Accounting performs month-end and year–end closing, maintains the chart of accounts, provides assistance and training to the local offices, and requests system changes from the Department of Information Technology (DIT). The Local Office Liaison Section of the Bureau of Accounting does not process or record any receipt or disbursement source documents other than when assisting a local office.

The LASR system is maintained by the Financial Applications Support Team and Relational Database Team of the DIT Application Software Development Division. User access to the application is provided through the FIA Office of Security and Financial Services.

The LASR system consists of an application (actually interconnected applications that for this purpose are considered to function as one application) and a database. Most LASR users only have access to the application. DIT staff that maintain the system have access to the database and may also have access to the application.

## SCOPE

We performed an audit of the general system controls and application controls for the period from July 10 through November 14, 2002.

We reviewed the following general controls:

- Controls over user access including user enrollment and the use of passwords.
- Controls over the system change process.
- Controls over the backup and recovery process.
- Controls over the use of the administrative rights in the database and in the application.

We reviewed the following application controls:

- Controls over data input, processing, error correction, and output from LASR.
- Proper separation of duties.

Note related to Application Controls

As indicated in the background section, LASR is operated as an individual stand-alone accounting system that supports the financial transactions within each local office. There are certain elements of application controls that are part of the LASR system (such as edits); but it is the processes and procedures within each local office that provide the application controls. The local office processes and procedures are reviewed in the local office audits performed by the Office of Internal Audit. The effect of any overall application controls information we found as part of this review will be considered during our local office audits. Any breakdowns in application controls are reported in the local office audits.

We met with both Bureau of Accounting Local Office Liaison Section staff, and the DIT Application Software Development Division staff. We obtained a description of the LASR system and reviewed some of the available system documentation. We obtained a description of, and evaluated the process for, making system changes and strategy for backup and recovery. We performed some limited testing of the system change process to supporting documentation. We reviewed the Accounting Manual and the Local Office Reports Description Manual. We obtained listings of user IDs and access rights and printouts of selected database tables related to access privileges and rights. We selected a sample of application users and traced the assigned rights to the supporting documentation.

## EXECUTIVE SUMMARY

Based on our review we conclude that the general controls that support the use and operation of the LASR application are not adequate to provide consistent and reliable information. Our report recommends that the number of users with system administrator rights be reduced to an appropriate number, that the ability to enroll application users be removed from the system administrator, and that programmers not be allowed to promote application changes into production. Our report also recommends that all database user IDs be associated with a specific individual, that the database and operating system user IDs not be shared, and that the operating system user IDs that need to be retained for installation or upgrade purposes be controlled by someone other than the database administrator. Our report also recommends that the process to obtain and remove user access to the LASR database be formalized and that a formal plan for purging, archiving, and restoring records be written.

Based on our review we concluded that there are certain central office located elements of application controls that are part of the LASR system (such as edits); but for the most part it is the processes and procedures within each local office that provide the application controls (or provide a compensating control for a system weakness). The local office processes and procedures are reviewed in the local office audits performed by the Office of Internal Audit. Therefore, we only reviewed certain application controls that were applicable to the FIA central office. Our report recommends that all application user IDs be associated with a specific individual who has submitted an access request with the proper approvals, the LR-890 User Responsibility Central Office report be reviewed and certified monthly by all central management staff that have LASR users to ensure that employee's access matches their current job requirements, and that only

requested access rights are granted, and that the Bureau of Accounting Local Office Liaison Section monitor the user access rights of central office users. Our report also recommends that no user be granted access to the application unless the enrollment form contains the proper approvals, that a separation of duties exist for LASR responsibilities that have the ability to input or approve a transaction, and that the LOL responsibility or any other application responsibility that is not inquire only be removed from the DIT staff who maintain the application or database. Overall, with the above exceptions we conclude that the application controls are adequate to ensure accurate, complete, and approved data, and that no unauthorized processing can occur. However, because of the weaknesses noted in the general controls, the application controls may be negated.

## AGENCY RESPONSE

FIA Budget, Analysis and Financial Management (BAFM) has reviewed all findings and recommendations included in this report. They indicated in a meeting held on May 7, 2003 that they are in general agreement with the report and will initiate the proper corrective action.

## FINDINGS AND RECOMMENDATIONS:

Excessive Number of Application System Administrators

1. The LASR system did not properly restrict system administrator rights. The LASR system has an excessive number of system administrators who are responsible for the integrity and operation of the application. System administrators can add, change, and delete information through the use of the application. Four individuals have these powerful administrative rights in the LASR system. Systems need one primary and one backup system administrator, and possibly others who may receive the rights in an emergency. A restricted

number of system administrators reduces the opportunity for inappropriate use of the administrative rights.

WE RECOMMEND that the office of Budget Analysis and Financial Management (BAFM) ensure that the number of users with system administrator access rights is reduced to one individual and a backup.

System Administrators can Enroll Users

2. The LASR system did not maintain the appropriate separation of duties over the granting of system access by ensuring that only the FIA Office of Security and Financial Services could enroll users on the system. All of the LASR system administrators can add users to the application through the use of the MFIA Security Enroll responsibility. LASR application users are required to submit an access request with the proper approvals to FIA Office of Security and Financial Services. However, system administrators who are located outside of the FIA Office of Security and Financial Services have the ability to enroll an application user without the required documentation and approvals.

WE RECOMMEND BAFM ensure that the ability to enroll application users is removed from the systems administrators and is limited to the FIA Office of Security and Financial Services.

Application Programmers can Promote System Changes to Production

3. The LASR system did not maintain the appropriate separation of duties over the promotion of system changes into production. To ensure that only authorized changes are introduced into the production environment the programmers responsible for writing the application system changes should not be able to move

the system changes into production. Three application programmers can promote system changes into production through the use of the MFIA Application Developer Reg responsibility.

WE RECOMMEND BAFM ensure that programmers are not allowed to promote application changes into production.

Application User ID not associated with a Person

4. The LASR system cannot provide accountability for all activity on the system or ensure that only authorized users have access to the system. In order to ensure accountability for all activity that occurs on a system and ensure that only authorized users have access, all application user IDs should be associated with a person who is an active employee. There are nine application user IDs on the system that are not associated with a person.

WE RECOMMEND that BAFM ensure that all application user IDs associated with a specific individual who has submitted an access request with the proper approvals to FIA Office of Security and Financial Services.

Database and Operating System User ID and Passwords

5. In addition to the nine application user IDs identified in Finding # 4 above, the LASR system cannot provide accountability for the database or operating system activity or enforce a separation of duties. None of the database user IDs and the operating system user IDs used to access the database and application files are associated with a specific person. In addition, these user IDs (and the passwords) are shared by database administrators, application system administrators, and a programmer/analyst.

- Accountability for any activity is not possible unless the user ID (and password) is associated with a specific person who is an active employee.
- A separation of duties between the Application System Administrator and the Database Administrator cannot be enforced if they share access.

WE RECOMMEND BAFM ensure that all database user IDs that are used to maintain the database are associated with a specific individual.

WE ALSO RECOMMEND that BAFM inform all LASR system users that database and operating system user IDs and passwords should not be shared.

WE FURTHER RECOMMEND that BAFM ensure that user IDs are controlled by someone other than the database administrators or others that maintain the database for operating system IDs that need to be retained for installation or upgrade purposes.

Application Users without a LASR SECURITY ACCESS REQUEST Form on File

6. The LASR system did not ensure that only authorized users have access to the application. Out of a sample of 149, 15 users did not have the required access enrollment form on file. Application users are required to submit an access request with the proper approvals to FIA Office of Security and Financial Services.

WE RECOMMEND BAFM ensure that all application users have an access request with the proper approvals on file in the FIA Office of Security and Financial Services.

User not End-dated

7. The LASR system did not ensure that access to the system was removed when a user no longer required access to perform their job functions. BAFM did not require Central Office Units to review the LR-890 User Responsibility Report to certify that all users listed on the report continue to be authorized. The user access for a contractor who had stopped working with the application in June or July of 2001 was not end-dated until July of 2002. The user access for a former database administrator had not been end-dated.

WE RECOMMEND BAFM require Central Office Units to review and certify the LR-890 User Responsibility Central Office Report monthly to ensure that employee's access matches their current job requirements.

No Formal Process to Gain Access to the Database

8. BAFM has not established a formal process to grant user access to the database. The database administrator grants user access to the database. No forms are required, there is no documentation of the need, and there is no documentation of approvals. In addition, because the database user IDs are not associated with a person and passwords are shared, there is no formal process to ensure that the database passwords are changed timely when one of the users that is sharing access no longer needs access.

WE RECOMMEND that BAFM formalize the process to grant and remove user access to the database.

WE ALSO RECOMMEND that BAFM require that users change their passwords on a regular basis.

Incorrect Application User Rights Assigned

9. Application users were assigned inappropriate user access rights. The access rights granted did not correspond to the requested access rights. Inappropriate user access rights could allow a user to process transactions that do not correspond to their job responsibility.

WE RECOMMEND that BAFM ensure that only requested access rights are granted.

Improper Approvals on the LASR SECURITY ACCESS REQUEST Forms

10. The LASR system did not ensure that only authorized users have access to the application. Two out of a sample of 149 LASR SECURITY ACCESS REQUEST forms did not contain the appropriate signatures. One of the forms was signed by the fiscal supervisor but should have been signed by the employee. The other had no supervisor's signature.

WE RECOMMEND BAFM ensure that no user be granted access to the application unless the enrollment form contains the correct signatures/approvals.

Record Purge and Archive Policy

11. BAFM has not formally established a record retention period, archived record storage location and medium, or a process for restoring archived records. In order to ensure that records are purged and archived in an orderly process, and that there is a process to restore archived records, there should be a formal plan in place.

WE RECOMMEND that BAFM develop a formal plan for purging, archiving, and restoring records.

User Responsibilities

12. LASR does not enforce a separation of duties if certain responsibilities within the application are granted to users. The AP INVOICE SUPV (create and approve an invoice) or GL JOURNAL ENTER SUPV (create and approve a journal entry) application responsibilities combine the ability to input and approve a transaction. Also, there is no transaction approval process for AR (accounts receivable). ACM sections 410 and 450 covering accounts payable and journal vouchers

respectively require that a hard copy of edit listings be printed and approved by a second person. Local office report LR-854 identifies invoices that were entered and approved by the same person. These compensating controls provide a measure of control, but are not as effective as a preventative system enforced control.

WE RECOMMEND that BAFM revise each responsibility to enable a user to either input or approve any particular type of transaction. No responsibility should have the ability to do both.

DIT Staff with LOL Responsibility

13. The LASR system did not maintain the appropriate separation of duties. Some DIT staff have the LOL application responsibility. The LOL responsibility is used by the Local Office Liaison Section manager of the Bureau of Accounting to maintain overall control of the financial processing done within the local offices. An appropriate separation of duties dictates that the DIT personnel responsible for maintaining the application should not have access to the application data.

WE RECOMMEND that BAFM remove the LOL responsibility or any other application responsibility that is not inquiry only from the DIT staff who maintain the application or database.